(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-509938
(P2005-509938A)
(43)公表日　平成17年4月14日(2005.4.14)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06F	15/00	G06F	15/00	330E	5B085
G06F	1/00	G06F	1/00	370E	5J104
H04L	9/08	H04L	9/00	673A	
H04L	9/32	H04L	9/00	601E	

審査請求 有　予備審査請求 有　（全 21 頁）

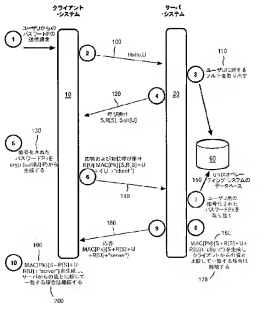
(21)出願番号　特願2003-544565(P2003-544565)
(86)(22)出願日　平成14年11月4日(2002.11.4)
(85)翻訳文提出日　平成16年5月7日(2004.5.7)
(86)国際出願番号　PCT/GB2002/004970
(87)国際公開番号　WO2003/042798
(87)国際公開日　平成15年5月22日(2003.5.22)
(31)優先権主張番号　10/007,859
(32)優先日　平成13年11月13日(2001.11.13)
(33)優先権主張国　米国(US)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】オペレーティング・システムの機能を用いて相互呼掛け応答認証プロトコルを実施する方法、機器およびコンピュータ・プログラム

(57)【要約】
【課題】サーバ処理が、暗号保護されたクライアント・パスワードを格納するリポジトリへのアクセス権を有する場合に使うためのクライアント－サーバ認証方法を提供すること。
【解決手段】本方法は、格納されている暗号保護されたクライアント・パスワードを生成するために予め適用されていたのと同じ暗号関数を、クライアントのパスワードのクライアント側コピーに適用することを含む。こうすることにより、クライアントおよびサーバ両方が、暗号保護された等しいクライアント・パスワードを利用することを保証する。すなわち、サーバ側でパスワードを平文に変換する必要なく、相互呼掛け応答認証プロトコルを実施するための共有の秘密を提供する。本発明は、ＵＮＩＸ（Ｒ）環境において重大な追加ソフトウェア基盤なしで実装することができる。クライアント・パスワードは通常、パスワードと乱数（「ソルト」）の組合せに適用されるcrypt()関数の保護の下で、ＵＮＩＸ（Ｒ）のパスワード・リポジトリに格納される。認証プロトコルのサーバの最初の呼掛けと共にソルトをクライアン



【特許請求の範囲】
【請求項１】
サーバ・データ処理システムが、暗号保護されたクライアント・パスワードを格納するリポジトリへのアクセス権を有する分散型データ処理環境のための認証方法であって、前記暗号保護されたクライアント・パスワードが、前記クライアント・パスワードに暗号関数を適用することによって生成されており、
前記格納されている暗号保護されたクライアント・パスワードに対応する前記クライアント・パスワードに前記暗号関数を適用することによって、前記格納されている暗号保護されたクライアント・パスワードに等しい、暗号保護されたクライアント・パスワードを生成する、クライアント・データ処理システムで処理すること、
クライアント・データ処理システムの暗号保護されたクライアント・パスワードと、前記サーバ・データ処理システムの、格納されている暗号保護されたクライアント・パスワードとを認証検査用の共有の秘密として用いて、前記認証検査を実施することを含む方法。
【請求項２】
前記認証検査が、相互呼掛け応答認証プロトコル検査を実施することを含む、請求項１に記載の方法。
【請求項３】
前記暗号関数が暗号化アルゴリズムである、請求項１に記載の方法。
【請求項４】
前記認証検査が、クライアント・データ処理システムおよび前記サーバ・データ処理システム両方において共通秘密セッション鍵を生成すること、前記クライアント側で、前記生成された暗号化されたクライアント・パスワードを使用し、前記サーバ側で、前記格納されている暗号化されたクライアント・パスワードを使用すること、ならびに、この共通秘密セッション鍵を相互呼掛け応答認証プロトコルにおいて使用することを含む、請求項３に記載の方法。
【請求項５】
前記共通秘密セッション鍵が、前記クライアントにおける前記生成された暗号化されたクライアント・パスワード、および前記サーバにおける前記格納されている暗号化されたクライアント・パスワードのそれぞれに暗号関数を適用することによって生成される、請求項４に記載の方法。
【請求項６】
前記暗号関数がハッシュ関数である、請求項１または２に記載の方法。
【請求項７】
前記リポジトリに格納された、暗号保護された各クライアント・パスワードが、それぞれのトークンと共に格納され、前記暗号保護されたクライアント・パスワードが、前記クライアント・パスワードを前記それぞれのトークンと組み合わせるとともに前記組合せに前記暗号関数を適用することによって生成され、
格納されている暗号保護されたクライアント・パスワードに対する前記それぞれのトークンを前記リポジトリから取り出し、クライアント・データ処理システムに前記トークンを送信する、前記サーバ・データ処理システムでの処理と、
前記送信されたトークン、および前記格納されている暗号保護されたパスワードに対応する前記クライアント・パスワードの前記組合せに前記暗号関数を適用することによって、前記等しい暗号保護されたクライアント・パスワードを、共有の秘密として使うために生成する、前記クライアント・データ処理システムでの前記処理とを含む、請求項１ないし６のいずれかに記載の方法。
【請求項８】
前記サーバ・データ処理システムのパスワード・リポジトリが、好ましくは前記サーバ・データ処理システムの前記オペレーティング・システム内に統合され、前記オペレーティング・システムが、ＵＮＩＸ（Ｒ）オペレーティング・システム標準に準拠し、または

ＵＮＩＸ（Ｒ）準拠のオペレーティング・システム派生のオペレーティング・システムである、請求項１ないし７のいずれかに記載の方法。

【請求項９】

前記暗号化アルゴリズムが、ＵＮＩＸ（Ｒ）のcrypt()関数によって提供される、請求項１０に記載の方法。

【請求項１０】

マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムであって、前記プログラム・コードが、相互呼掛け応答認証プロトコルに参加するサーバ処理を含み、前記サーバ処理が、クライアント・パスワードの暗号保護されたコピーを格納するリポジトリへのアクセス権を有し、前記暗号保護されたクライアント・パスワードが、前記クライアント・パスワードに第１の暗号関数を適用することによって生成されており、前記サーバ処理が、

実施すべき動作要求を指示するクライアント処理に応答して、サーバ呼掛けを生成し、前記サーバ呼掛けを前記クライアント処理に送信する手段であって、そうすることによって、前記クライアント処理が、

（ｉ）前記クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、前記クライアント処理および前記サーバ処理に共有の秘密を提供し、次いで、

（ｉｉ）前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成し、それを前記サーバ処理に転送することを可能にする手段と、

前記クライアント処理から前記クライアントの応答および対抗呼掛けを受信する手段と、

前記リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出す手段と、

前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、

一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、

前記サーバ応答を前記クライアント処理に転送して、前記クライアント処理が認証検査を実施することを可能にする手段とを備えるコンピュータ・プログラム。

【請求項１１】

マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムであって、前記プログラム・コードが、相互呼掛け応答認証プロトコルに参加するクライアント処理を含み、前記クライアント処理が、

サーバ処理に実施すべき動作要求を指示し、そうすることによって、前記サーバ処理がサーバ呼掛けを生成しそれを前記クライアント処理に送信するよう促す手段と、

前記クライアントのパスワードに暗号関数を適用して、暗号保護されたクライアント・パスワードを生成する手段と、

前記サーバ呼掛けの受信に応答して、前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成する手段と、

前記クライアントの応答および対抗呼掛けを前記サーバ処理に転送することを可能にする手段であって、そうすることによって、前記サーバ処理が、

（ｉ）前記クライアントの応答および対抗呼掛けを受信すること、

（ｉｉ）前記クライアントのパスワードに前記暗号関数を適用することによって生成された、暗号保護されたクライアント・パスワードを格納するリポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出すこと、

（ｉｉｉ）前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成すること、

（ｉｖ）前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定し、一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成し、前記サーバ応答を前記クライアント処理に転送することを促す手段と、

予期されるサーバ応答に対応するメッセージ認証コードを生成する手段と、

前記転送されたサーバ応答を受信する手段と、

前記転送されたサーバ応答および前記予期されるサーバ応答を比較して、２つの応答が一致するか判定する手段とを備えるコンピュータ・プログラム。

【請求項１２】

クライアント・パスワードの暗号保護されたコピーを格納するリポジトリであって、前記クライアント・パスワードが、第１の暗号関数を適用することによって生成されているリポジトリと、

関連づけられたクライアント・パスワードを有するクライアント処理との相互呼掛け応答認証プロトコルに参加するサーバ処理とを含むデータ処理システムであって、前記サーバ処理が、

実施すべき動作要求を指示するクライアント処理に応答して、サーバ呼掛けを生成し、前記サーバ呼掛けを前記クライアント処理に送信する手段であって、そうすることによって、前記クライアント処理が、

（ｉ）前記クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、前記クライアント処理および前記サーバ処理に共有の秘密を提供し、次いで、

（ｉｉ）前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、前記クライアントの応答および対抗呼掛けを生成し、それを前記サーバ処理に転送することを可能にする手段と、

前記クライアント処理から前記クライアントの応答および対抗呼掛けを受信する手段と、

前記リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出す手段と、

前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、

一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、

前記サーバ応答を前記クライアント処理に転送して、前記クライアント処理が認証検査を実施することを可能にする手段とを備えるデータ処理システム。

【請求項１３】

請求項１２に記載の第１のデータ処理システムと、クライアント・データ処理システムとを備える分散型データ処理システムであって、前記クライアント・データ処理システムがクライアント処理を含み、前記クライアント処理が、

前記クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、前記クライアント処理および前記サーバ処理に共有の秘密を提供すること、

前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、前記サーバ呼掛けに対するクライアントの応答および対抗呼掛けを生成すること、

前記クライアントの応答および対抗呼掛けを前記サーバ処理に転送すること、

前記転送されたサーバ応答を受信すること、
予期されるサーバ応答を生成し、前記受信したサーバ応答および前記予期されるサーバ応答を比較して、２つの応答が一致するか判定すること、ならびに、
肯定一致に応答して、認証を成功させることであるデータ処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ処理ネットワークにおける通信相手の認証に関する。
【背景技術】
【０００２】
相互呼掛け応答認証プロトコルは公知であり、ソフトウェア産業において広く実装されている。こうしたプロトコルは、クライアントおよびサーバそれぞれにおいて秘密セッション鍵の生成を必要とする。クライアントおよびサーバは、サーバ呼掛けならびにクライアントの応答および対抗呼掛けを介して、互いにこの秘密を知っていることを証明する。こうすることにより、クライアント－サーバ接続を（たとえば「介入者」が）スヌーブすることによってパスワードが発見されないように保護する。
【０００３】
相互呼掛け応答認証プロトコルの１つの変形体は、クライアントのパスワードを使った秘密セッション鍵の計算を含む。これには、クライアントのユーザＩＤおよびパスワードからなるデータベースへのアクセス権をサーバが有することが必要である。このプロトコルの多くの実装において、パスワードは、通信リンクの各端部において平文で保持される。平文パスワードを用いる典型的な認証プロトコルは、以下のように説明することができる。クライアントは、サーバに接続する。サーバは、それ自体をＳと識別し、乱数R_Sの「呼掛け」をクライアントに送信する。クライアントは、それ自体の識別情報Ｃ、それ自体が選択したR_Cの無作為呼掛け、およびメッセージ列{S+R_S+C+R_C+"Client"}というＭＡＣ（メッセージ認証コード）を用いて応答する。ＭＡＣは、クライアントのパスワードＰ$_C$をＭＡＣ鍵として使って計算される。（「＋」記号はここでは、ビット列の連結を表すのに使われている）。クライアントがそのパスワードを知っていることにサーバが納得した場合、サーバは、（同じ）パスワードＰ$_C$をＭＡＣ鍵として使って計算されたメッセージ列{S+R_S+C+R_C+"Server"}からなるＭＡＣを用いて応答することによって、サーバもパスワードを知っていることを証明する。これを、図１に表す。
【０００４】
このようなプロトコルは、「反射」攻撃および「リプレイ」攻撃を回避するように設計される。サーバがクライアントの呼掛けを満足させる前にクライアントがサーバの呼掛けを満足させなければならないので、クライアントを装う攻撃者は、「オフライン」でのパスワード推測攻撃を行うための情報を集めることができない。クライアントおよびサーバ両方がパスワードを知っていることを互いに証明するので、このプロトコルは、「扮装」攻撃に対する脆弱性がない。ＭＡＣで符号化されたストリングを誰かが傍受した場合でも、ストリングからパスワードを推測するのは計算が非常に難しく、したがって、クライアントまたはサーバに「なりすます」のは非常に難しい。
【０００５】
米国特許第５，８７２，９１７号は、パスワードを共有の秘密として用いる、通信相手の相互認証方法を開示している。認証の両当事者は、認証プロトコルのデータ交換中にパスワードを明らかにすることなく、共有パスワードを知っていることを証明する。
【０００６】
しかし、認証プロトコルにおいて使うために、パスワードを通信リンクの両端において平文で保持することは、依然として、こうした公知の解決法にとって機密の露出となる。ネットワークを介して送られたデータ列からの計算が難しいとしても、パスワードが（短時間ではあっても）平文の形でサーバ上に保持されるということは、機密を露出することになる。さらに、一部のオペレーティング・システムは、そのパスワード・データベース

からパスワードを平文の形で取り出すことを許可しない。

【０００７】

ケルベロス認証サービスや、公開鍵および秘密鍵認証を用いるＳＳＬ（セキュア・ソケット・レイヤ）など、より優れたレベルの安全性を提供する代替的な解決法は、その実装のために重要な追加ソフトウェア基盤、たとえば安全な追加パスワード・リポジトリの作成および維持を必要とする。さらに、ＳＳＬなど比較的安全な解決法は、単純なテルネットのようなパスワード認証など比較的脆弱な解決法よりも多くの計算資源を必要とする（すなわち、遅くなる傾向にある）。

【０００８】

こうした問題の結果、ＵＮＩＸ（Ｒ）システム上での相互呼掛け応答認証プロトコルの公知の実装には、重要な追加ソフトウェア基盤および処理時間が必要とされている（ＵＮＩＸ（Ｒ）はオープン・グループの登録商標である）。

【特許文献１】米国特許第５，８７２，９１７号

【発明の開示】

【発明が解決しようとする課題】

【０００９】

重要な追加ソフトウェア基盤を必要とすることなく、相互呼掛け応答パスワード認証プロトコルに対して向上した安全性を提供する必要がある。

【課題を解決するための手段】

【００１０】

第１の態様によると、本発明は、サーバ・データ処理システムが、暗号保護されたクライアント・パスワードを格納するリポジトリへのアクセス権を有する分散型データ処理環境における認証方法を提供し、クライアント・パスワードに暗号関数を適用することによって、暗号保護されたクライアント・パスワードが生成され、この認証方法は、格納されている暗号保護されたクライアント・パスワードに対応するクライアント・パスワードに同じ暗号関数を適用し、そうすることによって、格納されている暗号保護されたクライアント・パスワードに等しい暗号保護されたクライアント・パスワードを生成する、クライアント・データ処理システムでの処理、ならびに、クライアント・データ処理システムの暗号保護されたクライアント・パスワードと、サーバ・データ処理システムの、格納されている暗号保護されたクライアント・パスワードとを認証検査用の共有の秘密として用いて、前記認証検査を実施することを含む。

【００１１】

好ましくは、この認証検査は、相互呼掛け応答認証プロトコル検査の実施を含む。

【００１２】

暗号保護は、暗号化（この暗号化に置いて、暗号関数は、逆転用の復号キーを必要とする可逆の暗号化アルゴリズムである）やハッシュ化（このハッシュ化において、暗号関数は不可逆ハッシュ関数である）を含むどの形の暗号保護でもよい。クライアント処理およびサーバ処理は、一致した暗号関数を使用するように構成され、またはどの暗号関数を使うか交渉する。クライアント処理およびサーバ処理は、方法の第１段階としてこのクライアント用のパスワードを一致させ、サーバは、このパスワードを後で使うために格納する。

【００１３】

認証検査は好ましくは、（たとえば、暗号化されたパスワードをハッシュすることによって）暗号保護されたクライアント・パスワードから共通秘密セッション鍵を生成すること、および、相互呼掛け応答認証プロトコルにおいてこの共通秘密セッション鍵を使用することを含む。サーバ・データ処理システムのパスワード・リポジトリは好ましくは、サーバ・システムのオペレーティング・システムが所有するパスワード・リポジトリである。オペレーティング・システムは好ましくは、ＵＮＩＸ（Ｒ）オペレーティング・システム標準に準拠する、またはＵＮＩＸ（Ｒ）準拠のオペレーティング・システムから派生したオペレーティング・システムである（以下を参照されたい）。実際、暗号化アルゴリズ

ムが使われる場合、その暗号化アルゴリズムは、ＵＮＩＸ（Ｒ）のcrypt()関数によって提供することができる。

【００１４】

好ましくは、共通秘密セッション鍵は、クライアントにおいて生成された、暗号化されたクライアント・パスワード、および、サーバにおいて格納されている、暗号化されたクライアント・パスワードのそれぞれに暗号関数を適用することによって生成される。

【００１５】

好ましい実施形態によると、本発明は、サーバ・データ処理システムが、暗号保護されたクライアント・パスワード（たとえば、暗号化されたクライアント・パスワード）を格納するリポジトリへのアクセス権を有する分散型データ処理環境における認証方法を提供し、暗号保護された各クライアント・パスワードがそれぞれの乱数（「ソルト（salt）」）などのトークンと共に格納され、クライアント・パスワードをそれぞれのトークンと組み合わせるとともにこの組合せに暗号関数（たとえば暗号化アルゴリズム）を適用することによって暗号保護されたクライアント・パスワードが生成される。本方法は好ましくは、格納されている暗号保護されたクライアント・パスワードに対するそれぞれのトークンをリポジトリから取り出すとともにクライアント・データ処理システムにトークンを送信する、サーバ・データ処理システムでの処理、送信されたトークンと、格納されている暗号保護されたパスワードに対応するクライアント・パスワードとの組合せに暗号関数を適用し、そうすることによって、格納されている暗号保護されたクライアント・パスワードに等しい暗号保護されたクライアント・パスワードを生成する、クライアント・データ処理システムでの処理、ならびに、クライアント・データ処理システムの、暗号保護されたクライアント・パスワードと、サーバ・データ処理システムの、格納されている暗号保護されたクライアント・パスワードとを認証検査用の共有の秘密として用いることを含む。

【００１６】

本発明は特に、ＵＮＩＸ（Ｒ）オペレーティング・システム環境を実行するサーバ・データ処理システムに適用可能である。ＵＮＩＸ（Ｒ）は、オペレーティング・システムでもあり、オペレーティング・システム用のオープン・スタンダードでもある。ＵＮＩＸ（Ｒ）は最初、１９６９年にベル研究所で開発され、様々な企業、大学、および個人によって実現された多くの拡張および個別の実装により、オープン・スタンダードに発展した。ＵＮＩＸ（Ｒ）環境およびクライアント／サーバ・プログラム・モデルは、インターネット中心およびネットワーク中心の計算の発展において重要な要素であった。ＵＮＩＸ（Ｒ）ベースのオペレーティング・システムは、（たとえば、ＩＢＭコーポレーション、サン・マイクロシステムズおよび他数社から）広く販売されているワークステーション製品に使われている。Ｌｉｎｕｘオペレーティング・システムは、ＵＮＩＸ（Ｒ）派生であり、所有権のあるオペレーティング・システムに代わるものとして、人気が高まっている。本明細書では、わかりやすくするために、ＵＮＩＸ（Ｒ）オペレーティング・システムをベースとし、またはそれから派生した、あるいはＵＮＩＸ（Ｒ）オペレーティング・システム標準に準拠するすべてのオペレーティング・システムを、例として「ＵＮＩＸ（Ｒ）オペレーティング・システム」と呼ぶ。

【００１７】

本発明における重要な見識は、サーバでのＵＮＩＸ（Ｒ）オペレーティング・システムのパスワード・リポジトリに格納する前に、パスワードに適用される暗号関数を知ることによって、クライアントが、サーバ上で既に保持されているパスワードに等しい暗号保護されたパスワードを計算できるようになると発明者達が認識していることである。たとえば、ＵＮＩＸ（Ｒ）標準に準拠する多くのオペレーティング・システムは、パスワードと乱数すなわち「ソルト」との組合せに適用される広く使用可能なcrypt()関数を使い、Ｌｉｎｕｘオペレーティング・システムはハッシュ関数を使う。暗号保護されたパスワードの格納され計算されたコピーは、直接、またはセッション鍵の生成元である共有の秘密を提供することによって、共通秘密セッション鍵を提供し、その鍵を用いて相互呼掛け応答認証プロトコルを実行する。

【００１８】
このように、既存のパスワード・リポジトリから引き出された、暗号保護されたパスワードを利用できることにより、クライアント・パスワードをサーバ上で平文に復号するようにという、受信した要求に関連して機密が露出されることを回避するとともに、他の公知の解決法による追加のソフトウェア基盤の要求も回避する。
【００１９】
本発明は、コンピュータ・プログラムまたは１組のコンピュータ・プログラム構成要素として実装することができ、上述した方法を実施するための、１つまたは複数のコンピュータ可読記録媒体（たとえば磁気または光学媒体）に記録されたプログラム・コードを備える。
【００２０】
さらなる態様では、本発明は、分散型クライアント－サーバ・データ処理システムにおける相互呼掛け応答認証のためのクライアント処理およびサーバ処理それぞれを提供し、それぞれのクライアント処理およびサーバ処理を含むクライアント・データ処理システムおよびサーバ・データ処理システムそれぞれを提供する。
【００２１】
サーバ処理は、クライアント・パスワードの暗号保護されたコピーを格納するリポジトリへのアクセス権を有し、暗号保護されたクライアント・パスワードは、クライアント・パスワードに第１の暗号関数を適用することによって生成されている。サーバ処理は、実施すべき動作要求を指示するクライアント処理に応答して、サーバ呼掛けを生成し、サーバからのこの呼掛けをクライアント処理に送信することができる。クライアント処理は次いで、クライアントのパスワードに同じ暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成することができる。こうすることにより、クライアントおよびサーバ処理に共有の秘密を提供する。次いで、クライアント処理は、暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成し、それをサーバ処理に転送することができる。サーバ処理は、クライアント処理からクライアントの応答および対抗呼掛けを受信する。サーバ処理は、リポジトリにアクセスして、格納されている暗号保護されたクライアント・パスワードを取り出し、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを（前記格納されている暗号保護されたクライアント・パスワードを使って）生成する。サーバ処理は次いで、受信したメッセージ認証コードと生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する。一致に応答して、サーバ処理は、クライアントの応答および対抗呼掛けに対するサーバ応答を生成し、この応答をクライアント処理に転送して、クライアント処理が認証検査を実施することを可能にする。
【００２２】
一態様によると、本発明は、マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムを提供し、プログラム・コードは、相互呼掛け応答認証プロトコルに参加するサーバ処理を含み、サーバ処理は、クライアント・パスワードの暗号保護されたコピーを格納するリポジトリへのアクセス権を有し、暗号保護されたクライアント・パスワードは、クライアント・パスワードに第１の暗号関数を適用することによって生成されており、サーバ処理は、実施すべき動作要求を指示するクライアント処理に応答して、サーバ呼掛けを生成し、サーバからのこの呼掛けをクライアント処理に送信する手段であって、そうすることによって、クライアント処理が、
（ｉ）クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、クライアント処理およびサーバ処理に共有の秘密を提供し、次いで、
（ｉｉ）暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成し、それをサーバ処理に転送することを可能にする手段と、

クライアント処理からクライアントの応答および対抗呼掛けを受信する手段と、リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出す手段と、前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、受信したメッセージ認証コードおよび生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、一致に応答して、クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、サーバ応答をクライアント処理に転送して、クライアント処理が認証検査を実施することを可能にする手段とを備える。

【００２３】

別の態様によると、本発明は、マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムを提供し、プログラム・コードは、相互呼掛け応答認証プロトコルに参加するクライアント処理を含み、クライアント処理は、サーバ処理に実施すべき動作要求を指示し、そうすることによって、サーバ処理がサーバ呼掛けを生成しそれをクライアント処理に送信するよう促す手段と、クライアントのパスワードに暗号関数を適用して、暗号保護されたクライアント・パスワードを生成する手段と、サーバ呼掛けの受信に応答して、暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成する手段と、クライアントの応答および対抗呼掛けをサーバ処理に転送することを可能にする手段であって、そうすることによって、サーバ処理が、

（ｉ）クライアントの応答および対抗呼掛けを受信すること、

（ｉｉ）クライアントのパスワードに前記暗号関数を適用することによって生成された、暗号保護されたクライアント・パスワードを格納するリポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出すこと、

（ｉｉｉ）前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成すること、

（ｉｖ）受信したメッセージ認証コードおよび生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定し、一致に応答して、クライアントの応答および対抗呼掛けに対するサーバ応答を生成し、サーバ応答をクライアント処理に転送することを促す手段と、

予期されるサーバ応答に対応するメッセージ認証コードを生成する手段と、転送されたサーバ応答を受信する手段と、転送されたサーバ応答および予期されるサーバ応答を比較して、２つの応答が一致するか判定する手段とを備える。

【００２４】

さらなる態様によると、本発明は、クライアント・パスワードの暗号保護されたコピーを格納するリポジトリであって、クライアント・パスワードに第１の暗号関数を適用することによって暗号保護されたクライアント・パスワードが生成されているリポジトリと、関連づけられたクライアント・パスワードを有するクライアント処理との相互呼掛け応答認証プロトコルに参加するサーバ処理とを含むデータ処理システムを提供し、サーバ処理は、実施すべき動作要求を指示するクライアント処理に応答して、サーバ呼掛けを生成し、サーバからのこの呼掛けをクライアント処理に送信する手段であって、そうすることによって、クライアント処理が、

（ｉ）クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、クライアント処理およびサーバ処理に共有の秘密を提供し、次いで、

（ｉｉ）暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成し、それをサーバ処理に転送することを可能にする手段と、

クライアント処理からクライアントの応答および対抗呼掛けを受信する手段と、リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出

す手段と、前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、受信したメッセージ認証コードおよび生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、一致に応答して、クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、サーバ応答をクライアント処理に転送して、クライアント処理が認証検査を実施することを可能にする手段とを備える。

【００２５】

別の態様によると、本発明は、上記の段落による第１のデータ処理システムと、クライアント・データ処理システムとを備える分散型データ処理システムを提供し、クライアント・データ処理システムは、クライアント処理を含み、この処理は、クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、クライアント処理およびサーバ処理に共有の秘密を提供すること、暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、サーバ呼掛けに対するクライアントの応答および対抗呼掛けを生成すること、クライアントの応答および対抗呼掛けをサーバ処理に転送すること、転送されたサーバ応答を受信すること、予期されるサーバ応答を生成し、受信したサーバ応答および予期されるサーバ応答を比較して、２つの応答が一致するか判定すること、ならびに、肯定一致に応答して、認証を成功させることである。

【００２６】

本発明の好ましい実施形態を、例示の目的のために、添付の図面を参照して以下でより詳しく説明する。

【発明を実施するための最良の形態】

【００２７】

上述したように、図１は、典型的な相互呼掛け応答パスワード認証プロトコルを表す。本発明の好ましい実施形態によると、このようなプロトコルは、サーバにおいてパスワードを平文で露出することなく、また、追加のソフトウェア基盤を必要とせずに、展開することができる。具体的には、追加のパスワード・データベースの作成および維持は必要ない。そうではなく、ＵＮＩＸ（Ｒ）オペレーティング・システム機能が利用される。

【００２８】

図２は、サーバ・データ処理システム２０への通信リンク３０を有するクライアント・データ処理システム１０を示す。当該分野で公知であるように、クライアント－サーバという枠組みは、関与しているデータ処理システムの性質に対するどのような限定も意味していない。そうではなく、２つのシステム上で実行されている処理の間の現在の関係を示す。すなわち、現在のタスクの場合、クライアント処理４０は、サーバ処理５０に対してサービスを要求している。サーバ・データ処理システムは、どのデータ処理システムでもよいが、ＵＮＩＸ（Ｒ）オペレーティング・システム（上述したように、これは、ＵＮＩＸ（Ｒ）オペレーティング・システムもしくは標準をベースとし、それから派生し、またはそれに準拠するどのオペレーティング・システムも含む）を実行することが好ましい。クライアント・データ処理システムもやはりどのシステムでもよく、具体的には、インターネット、イントラネット、または他のどのローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、モバイル・ネットワーク、電線網を介してもサーバに接続される、デスクトップ型ワークステーションでも、可搬型コンピュータ（あるいは、限られたメモリもしくは処理資源またはその両方を有するＰＤＡ）でもよい。

【００２９】

相互呼掛け応答認証プロトコルは、クライアントおよびサーバそれぞれにおいて秘密セッション鍵の生成を要求する。クライアントおよびサーバは、サーバ呼掛けと、クライアントの応答および対抗呼掛けとを介して、この秘密を知っていることを互いに証明する。

【００３０】

サーバは、ＵＮＩＸ（Ｒ）オペレーティング・システムが所有するパスワード・リポジトリに格納されている暗号化されたパスワードから、サーバの秘密セッション鍵を計算す

る。暗号化された等しいパスワードが、クライアントにおいて、ＵＮＩＸ（Ｒ）のcrypt()システム・コールまたは等価物をクライアントの平文パスワードに適用して計算される。次いで、こうした暗号化されたパスワードから、共通秘密セッション鍵を生成することができ、この鍵を用いて、相互呼掛け応答プロトコルを実施する。

【００３１】

crypt()関数の実装が様々なプラットフォーム上で広く利用可能であることにより、広範囲のクライアント・プラットフォームによってこのプロトコル実装をサポートすることが可能になる。クライアントは、暗号化されたパスワードのハッシュを生成することもできる。したがって、好ましい本実施形態においてクライアントに対して要求されることは、サーバにおいてクライアント・パスワードに適用された暗号化と一致するように平文パスワードを暗号化する方法と、呼掛けの要素をハッシュする方法がすべてである。crypt()関数は、両方に対して使うことができる。

【００３２】

平文パスワードは、サーバで格納される必要は全くない。したがって、複雑な追加クライアント基盤を必要とすることなく、少なくとも既存のＵＮＩＸ（Ｒ）の安全性によって保証される機密のレベルが維持される。この解決法はしたがって、既存の技術を用いて実装するのが容易である。

【００３３】

ＵＮＩＸ（Ｒ）オペレーティング・システムは、暗号化した形でパスワードを格納するが、その取出しのためのインターフェースも提供する。たとえばgetpwent()システム・コールは、指定されたユーザ名に対する暗号化されたパスワードを取り出す。ＵＮＩＸ（Ｒ）オペレーティング・システムによって使われる、平文パスワードから暗号化されたパスワードを生成するためのＤＥＳ暗号化に基づく機構が、Ｕｎｉｘ（Ｒ）のcrypt()システム・コールにおいて公表されている。crypt()関数は、２つのパラメータ、すなわち平文パスワードと、暗号化アルゴリズムによって使われる「ソルト」として知られる２文字（１２ビット）の乱数とを必要とする。その結果生じる、サーバにおいてuser/passwordリポジトリに格納される暗号化されたパスワードの先頭には、常に２文字のソルトがつく。

【００３４】

ソルトの目的は、何者かが暗号化されたパスワードのファイル全体に対するアクセス権を得て、「辞書攻撃」を行っている状況において、オフラインのパスワード推測を大幅に遅くさせることである。辞書攻撃とは、辞書にあるすべての語をハッシュし、パスワードのどれかが、格納されているハッシュ値のどれかと一致するか検査することである。ソルトがあっても、あるユーザのパスワードの推測を困難にするわけではないが、一度のハッシュ操作を実施するだけで、あるパスワードが一群のユーザの誰かに対して有効であるか調べることができないようにする。

【００３５】

crypt()は、パスワードおよびソルトを入力として受け取る。暗号化されたパスワードは、秘密鍵に変換される。ソルトは、修正ＤＥＳアルゴリズムを定義するのに用いられ、このアルゴリズムは、秘密鍵とともに使われて、ハッシュをもたらすために定数値を暗号化する。

【００３６】

次に、本発明の好ましい実施形態によるイベントの順序および情報の流れを、図３を参照して説明する。以下は、図３のシステムの間を流れる情報項目に関する鍵である。

・Ｕ－ユーザ識別子
・Ｐ－ユーザＵ用の平文パスワード
・Ｒ[Ｕ]－クライアントからの無作為呼掛け
・Ｓａｌｔ[Ｕ]－ユーザＵ用のソルト
・Ｓ－サーバ識別子
・Ｒ[Ｓ]－サーバからの無作為呼掛け
・Ｐｋ－ユーザＵ用の暗号化されたパスワード

・MAC[Pk]{str}－PkをＭＡＣ鍵として使って計算された、ストリングstrからなるメッセージ認証コード（ＭＡＣ）。

【００３７】

たとえばクライアント・データ処理システム上で実行される利用者のアプリケーション・プログラムが、サーバ上で実行される発行／引用メッセージ・ブローカからの発行を受けるために、そのブローカに登録することを望む場合、クライアント・システム上で実行される処理はサーバと通信が確立されるよう要求すると仮定する。クライアントおよびサーバは両方とも、安全なデータの通信を始めることができるようになる前に、他方のシステムの何らかの認証または処理を要求することができる。これは、発行すべき特定のデータが、無許可のアクセスからサーバ・システムを保護するために機密である、または支払済みのユーザだけが高額な資源にアクセスすることを保証するため、などの理由からである。

【００３８】

最初に、クライアント・データ処理システム上で実行される処理は、１００でサーバと交信し、クライアント識別情報をサーバに流す。サーバは次いで、１１０で、暗号化された適切なパスワードをＵＮＩＸ（Ｒ）オペレーティング・システムから抽出し、１２０で、先頭に追加されたソルトを、その呼掛けの一部としてクライアントに流す。クライアントは次いで、１３０で、その平文パスワードおよび受信したソルトに対してcrypt()を呼び出すことによって、呼掛け応答プロトコルのその他の部分を実行するために秘密セッション鍵を生成することができる。

【００３９】

クライアントは、１４０で、その応答および対抗呼掛けをサーバに送る。これは、暗号化されたパスワードをＭＡＣ鍵として用いて計算された、クライアントからの無作為呼掛けおよびストリング{S+R[S]+U+R[U]+"client"}からなるメッセージ認証コード（ＭＡＣ）を含む。サーバは、１５０で、現在のユーザ用の暗号化されたパスワードをＵＮＩＸ（Ｒ）オペレーティング・システムのuser/passwordデータベースから取り出し、このパスワードを使って、１６０で、メッセージ認証コードMAC[Pk]{S+R[S]+U+R[U]+"client"}を生成する。このコードは次いで、１７０で、クライアントから受け取った値と比較される。一致する場合、サーバは認証を成功とみなし、従って、認証プロトコルの通信フローは継続することができる。

【００４０】

メッセージ認証コードMAC[Pk]{S+R[S]+U+R[U]+"server"}を含む応答が、１８０で、クライアントに返送される。等しいメッセージ認証コードMAC[Pk]{S+R[S]+U+R[U]+"server"}も、１９０で、クライアント側で計算され、２００で、着信ＭＡＣと比較される。この２つが一致する場合、両端において認証が成功しており、通信を継続することができる。

【００４１】

この認証プロトコルは、発行／引用メッセージ・ブローカ製品による使用のために利用可能になっている、選び抜かれたプロトコルの１つとして実装することができる。ブローカは、異なる目的または異なるユーザに対して異なる認証プロトコルを使うように構成することができる。というのは、異なる顧客シナリオは、異なる安全性要件および他の性能要件、または解決アーキテクチャ要件を有する場合があるからである。

【００４２】

たとえば、本発明を実装する発行／引用メッセージ・ブローカは、以下のプロトコルの組をサポートすることができる。

ｉ．単純なテルネットのようなパスワード認証

ｉｉ．相互呼掛け応答パスワード認証

ｉｉｉ．サーバの公開鍵認証およびクライアントのパスワード認証を伴うＳＳＬ（セキュア・ソケット・レイヤ）「混成」

ｉｖ．サーバおよびクライアントの公開鍵認証を伴うＳＳＬ「純正」

【００４３】

こうしたプロトコルは、「攻撃」に対する強さ（すなわち、ｉの場合は比較的弱く、ｉｖの場合は比較的強い）、必要とされる「基盤」（ｉおよびｉｉの場合はほとんど必要とされず、ｉｖの場合はかなり必要とされる）、および必要とされる計算資源の点（すなわち、認証性能はｉでは「速い」が、ｉｖでは「比較的遅い」）において異なる。

【００４４】

この場合、ブローカ・ネットワークによる認証プロトコルの使用は、設定可能である。

・ブローカは、（ａ）０個のプロトコル、（ｂ）１個のプロトコル、または（ｃ）１組のプロトコルのいずれかをサポートするように構成することができる。

・クライアントも同様に、（ａ）０個のプロトコル、（ｂ）１個のプロトコル、または（ｃ）１組のプロトコルのいずれかをサポートするように構成することができる。

・異なるクライアントは、異なるプロトコルと同じブローカに接続されるように構成することができる（クライアントとサーバが、使用する認証プロトコルについて「交渉する」）。

・「最低強度」プロトコルは、ある特定のユーザまたは１組のユーザ用に、あるいはある特定の発行／引用トピック用に指定することができる。

【００４５】

ある顧客が、テストまたは評価環境用にあるレベルの安全性を要求し、製品化環境用には異なるレベルの安全性を要求する場合があり得る。他の顧客は、ローカル・ユーザがあるプロトコルを介してブローカに接続されることを要求する場合があり、インターネットを介してブローカにアクセスすることを望むユーザは、より強いプロトコルを使用する。顧客の要求は時間によっても変わる場合があり、設定可能な幅広い認証選択肢を実装する解決法により、顧客が自分のブローカ環境に適切に適応できるようになる。高性能を要求する顧客は、より弱いプロトコルを選び、他の手段によって自分の環境を安全にする場合もあり得る。

【００４６】

上で詳しく説明した相互呼掛け応答プロトコルはしたがって、コンピュータ・プログラム製品において、幅広い認証プロトコルの中の（安全性強度、計算要件、および管理用オーバーヘッドにおいて）「中程度の」選択肢として提供することができる。このプロトコルが存在することによって、解決法全体が強化され、プロトコルの再設定を容易にすることによって、こうしたプロトコルを使う可能性が高まる。

【図面の簡単な説明】

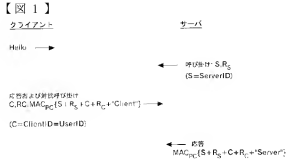
【００４７】

【図１】典型的な相互呼掛け応答認証プロトコルを示す図である。

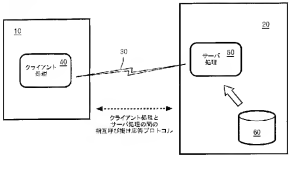
【図２】本発明を実装することができるクライアント－サーバ・データ処理環境を示す概略図である。

【図３】本発明の実施形態による認証プロトコルを示す図である。

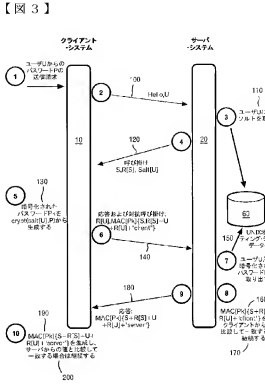
【図１】



【図２】



【図３】



【手続補正書】
【提出日】平成16年3月23日(2004.3.23)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１
【補正方法】変更
【補正の内容】
【請求項１】
サーバ・データ処理システムが、暗号保護されたクライアント・パスワードを格納するリポジトリへのアクセス権を有する分散型データ処理環境のための認証方法であって、前記リポジトリが、前記サーバ・データ処理システムのオペレーティング・システムと統合され、前記暗号保護されたクライアント・パスワードが、前記サーバ・データ処理システムのオペレーティング・システムによって提供される暗号関数を前記クライアント・パスワードに適用することによって生成されており、
前記格納されている暗号保護されたクライアント・パスワードに対応する前記クライアント・パスワードに前記暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成する、クライアント・データ処理システムでの処理であって、前記暗号関数もやはり前記サーバ・データ処理システムのオペレーティング・システムによって提供される処理、
前記クライアント・データ処理システムの暗号保護されたクライアント・パスワードと、前記サーバ・データ処理システムの、格納されている暗号保護されたクライアント・パスワードとを認証検査用の共有の秘密として用いて、前記認証検査を実施することを含む方法。
【手続補正２】
【補正対象書類名】特許請求の範囲

【補正対象項目名】請求項８
【補正方法】変更
【補正の内容】
【請求項８】
前記オペレーティング・システムが、ＵＮＩＸ（Ｒ）オペレーティング・システム標準に準拠し、またはＵＮＩＸ（Ｒ）準拠のオペレーティング・システム派生のオペレーティング・システムである、請求項１ないし７のいずれかに記載の方法。
【手続補正３】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項９
【補正方法】変更
【補正の内容】
【請求項９】
前記暗号化アルゴリズムが、ＵＮＩＸ（Ｒ）のcrypt()関数によって提供される、請求項８に記載の方法。
【手続補正４】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１０
【補正方法】変更
【補正の内容】
【請求項１０】
マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムであって、前記プログラム・コードが、相互呼掛け応答認証プロトコルに参加するオペレーティング・システムを有するサーバ・データ処理システム上で実行されるサーバ処理を含み、前記サーバ処理が、クライアント・パスワードの暗号保護されたコピーを格納するリポジトリへのアクセス権を有し、前記リポジトリが、前記サーバ・データ処理システムのオペレーティング・システムと統合され、前記暗号保護されたクライアント・パスワードが、前記サーバ・データ処理システムのオペレーティング・システムによって提供される暗号関数を前記クライアント・パスワードに適用することによって生成されており、前記サーバ処理が、
実施すべき動作要求を指示する、クライアント・データ処理システムでのクライアント処理に応答して、サーバ呼掛けを生成し、前記サーバ呼掛けを前記クライアント処理に送信する手段であって、そうすることによって、前記クライアント処理が、
（ｉ）やはり前記サーバ・データ処理システムのオペレーティング・システムによって提供される前記第１の暗号関数を前記クライアントのパスワードに適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、前記クライアント処理および前記サーバ処理に共有の秘密を提供し、次いで、
（ｉｉ）前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成し、それを前記サーバ処理に転送することを可能にする手段と、
前記クライアント処理から前記クライアントの応答および対抗呼掛けを受信する手段と、
前記リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出す手段と、
前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、
一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、

前記サーバ応答を前記クライアント処理に転送して、前記クライアント処理が認証検査を実施することを可能にする手段とを備えるコンピュータ・プログラム。
【手続補正５】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１１
【補正方法】変更
【補正の内容】
【請求項１１】
マシン可読記録媒体に記録されたプログラム・コードを備えるコンピュータ・プログラムであって、前記プログラム・コードが、相互呼掛け応答認証プロトコルに参加するクライアント処理を含み、前記クライアント処理が、オペレーティング・システムを有するクライアント・データ処理システムにおいて実行され、前記クライアント処理が、
オペレーティング・システムを有するクライアント・データ処理システムにおいて実行されるサーバ処理に実施すべき動作要求を指示し、そうすることによって、前記サーバ処理がサーバ呼掛けを生成しそれを前記クライアント処理に送信するよう促す手段と、
前記クライアントのパスワードに暗号関数を適用して、暗号保護されたクライアント・パスワードを生成する手段であって、前記暗号関数が、前記クライアント・データ処理システムの前記オペレーティング・システムによって提供される手段と、
前記サーバ呼掛けの受信に応答して、前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、クライアントの応答および対抗呼掛けを生成する手段と、
前記クライアントの応答および対抗呼掛けを前記サーバ処理に転送することを可能にする手段であって、そうすることによって、前記サーバ処理が、
（ｉ）前記クライアントの応答および対抗呼掛けを受信すること、
（ｉｉ）前記クライアントのパスワードに前記暗号関数を適用することによって生成された、暗号保護されたクライアント・パスワードを格納するリポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出すことであって、前記リポジトリが、前記サーバ・データ処理システムの前記オペレーティング・システムと統合され、前記暗号関数がやはり前記サーバ・データ処理システムの前記オペレーティング・システムによって提供されること、
（ｉｉｉ）前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成すること、
（ｉｖ）前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定し、一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成し、前記サーバ応答を前記クライアント処理に転送することを促す手段と、
予期されるサーバ応答に対応するメッセージ認証コードを生成する手段と、
前記転送されたサーバ応答を受信する手段と、
前記転送されたサーバ応答および前記予期されるサーバ応答を比較して、２つの応答が一致するか判定する手段とを備えるコンピュータ・プログラム。
【手続補正６】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１２
【補正方法】変更
【補正の内容】
【請求項１２】
オペレーティング・システムと、
クライアント・パスワードの暗号保護されたコピーを格納するとともにデータ処理システムの前記オペレーティング・システムと統合されているリポジトリであって、前記クラ

イアント・パスワードが、第１の暗号関数を適用することによって生成され、前記第１の暗号関数が、前記データ処理システムの前記オペレーティング・システムによって提供されるリポジトリと、

関連づけられたクライアント・パスワードを有するクライアント処理との相互呼掛け応答認証プロトコルに参加するサーバ処理とを含むデータ処理システムであって、前記サーバ処理が、

実施すべき動作要求を指示する、クライアント・データ処理システムでのクライアント処理に応答して、サーバ呼掛けを生成し、前記サーバ呼掛けを前記クライアント処理に送信する手段であって、そうすることによって、前記クライアント処理が、

（ｉ）前記クライアントのパスワードに前記第１の暗号関数を適用することによって、暗号保護されたクライアント・パスワードを生成し、そうすることによって、前記クライアント処理および前記サーバ処理に共有の秘密を提供することであって、前記第１の暗号関数がやはり前記クライアント・データ処理システムの前記オペレーティング・システムによって提供されること、次いで、

（ｉｉ）前記暗号保護されたクライアント・パスワードを使って計算されたメッセージ認証コードを含む、前記クライアントの応答および対抗呼掛けを生成し、それを前記サーバ処理に転送することを可能にする手段と、

前記クライアント処理から前記クライアントの応答および対抗呼掛けを受信する手段と、

前記リポジトリにアクセスし、前記格納されている暗号保護されたクライアント・パスワードを取り出す手段と、

前記格納されている暗号保護されたクライアント・パスワードを使って、予期されるクライアントの応答および対抗呼掛けに対応するメッセージ認証コードを生成し、前記受信したメッセージ認証コードおよび前記生成されたメッセージ認証コードを比較して、２つのコードが一致するか判定する手段と、

一致に応答して、前記クライアントの応答および対抗呼掛けに対するサーバ応答を生成する手段と、

前記サーバ応答を前記クライアント処理に転送して、前記クライアント処理が認証検査を実施することを可能にする手段とを備えるデータ処理システム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Internal application No
PCT/GB 02/04970

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	THOMAS WU: "The SRP Authentication and Key Exchange System" RFC2945, 'Online! 30 September 2000 (2000-09-30), XP002258525 Retrieved from the Internet: <URL:www.ietf.org/rfc/rfc2945.txt> 'retrieved on 2003-10-20! Chapter 3. The SRP-SHA1 mechanism page 3 -page 4 -/--	1-8, 10-13

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance
'E' earlier document but published on or after the international filing date
'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
'O' document referring to an oral disclosure, use, exhibition or other means
'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 October 2003	05/11/2003
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Alecu, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat application No
PCT/GB 02/04970

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
X	JABLON D P: "Extended password key exchange protocols immune to dictionary attack" ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES, 1997. PROCEEDINGS., SIXTH IEEE WORKSHOPS ON CAMBRIDGE, MA, USA 18-20 JUNE 1997, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 18 June 1997 (1997-06-18), pages 248-255, XP010253331 ISBN: 0-8186-7967-0 the whole document	1-8, 10-13
E	US 6 539 479 B1 (WU THOMAS J) 25 March 2003 (2003-03-25) column 3, line 32 - line 37 column 5, line 46 -column 6, line 14 column 7, line 41 -column 9, line 67 column 12, line 1 - line 39	1-8, 10-13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB 02/04970

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6539479 B1	25-03-2003	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(特許庁注：以下のものは登録商標)
Ｌｉｎｕｘ

(72)発明者 アストレイ、マーク
アメリカ合衆国０７４４２ ニュージャージー州ポンプトン・レイクス ビーコン・ヒル １８
(72)発明者 ヤング、ニール、ジョージ、スタンレイ
イギリス ＳＯ１７ １ＤＷ ハンプシャー州 サザンプトン ハイフィールド ブレンハイム・アベニュー ４１

Ｆターム(参考) 5B085 AE09 AE23 BE04 BG02 BG07
5J104 AA07 AA16 EA03 EA18 JA01 JA03 KA01 KA03 KA04 NA02
NA05 NA12 NA38 PA07

【要約の続き】
ト・システムに送ることによって、クライアント側の処理は、同じソルトを有するクライアント・パスワードにcrypt()関数を適用することができ、そうすることによって、クライアントおよびサーバは、認証用の共通セッション鍵として使うための共有の秘密をもつことができ、またはこの鍵を生成することができる。